

## REMARKS

Claims 1, 2, 4-10, 12-16 and 23-25 are amended herein. Claims 17-22 are canceled. Claims 1-16 and 23-25 are pending.

### Claim Objections

Claim 2 is objected to because of the cited informality. Claim 2 is amended herein to overcome the objection.

### 102 Rejections

Claims 1-5 and 9-13 are rejected under 35 U.S.C. § 102(e) as being anticipated by Khan et al. ("Khan;" US 6,401,206). The Applicants have reviewed the cited reference and respectfully assert that Khan does not show or suggest the embodiments of the present invention recited in Claims 1-5 and 9-13.

Independent Claim 1 recites that an embodiment of the present invention is directed to a "method of activating a smart card, comprising: receiving identifying information for a non-activated smart card; receiving manual authentication information for user to whom the non-activated smart card has been issued; authenticating the user and the non-activated smart card using the identifying information and the manual authentication information; obtaining a public key from the non-activated smart card; and issuing a digital certificate that is generated using the public key, wherein the non-activated smart card is activated upon receiving the digital certificate." Claims 2-5 are dependent on Claim 1.

Independent Claim 9 recites that an embodiment of the present invention is directed to a "method of activating a smart card, comprising: sending, to an administration server, identifying information read from a non-activated smart card; sending, to the administration server, manual authentication information input by a user to whom the non-activated smart card has been issued; generating a public key using the non-activated smart card; sending the public key to the administration server; and receiving a digital certificate that is generated using the public key, wherein the non-activated smart card is activated upon receipt of the digital certificate." Claims 10-13 are dependent on Claim 9.

Applicants respectfully assert that Khan does not show or suggest the present invention as recited in independent Claims 1 and 9. Applicants understand Khan to only describe the creation of a "digital identity" that perhaps can be used in a smart card. At best, the "digital identity" of Khan is possibly analogous to a digital certificate. However, the present claimed invention is not solely a method of creating a digital certificate. As recited in the claims, the present invention pertains to methods of activating a smart card. Applicants respectfully submit that Khan does not show or suggest a method of activating a smart card, and in particular does not show or suggest the methods of activating a smart card recited by Claims 1 and 9.

In summary, Applicants respectfully submit that Khan does not show or suggest the present invention as recited in independent Claims 1 and 9, and that Claims 1 and 9 traverse the Examiner's basis for rejection

under 35 U.S.C. § 102(e). Applicants also respectfully submit that Claims 2-5 (dependent on Claim 1) and Claims 10-13 (dependent on Claim 9) traverse the Examiner's basis for rejection under 35 U.S.C. § 102(e) as these claims are dependent on allowable base claims and recite additional limitations.

### 103 Rejections

Claims 6, 7, 8, 14, 15 and 16 are rejected under 35 U.S.C § 103(a) as being unpatentable over Khan in view of Boroditsky et al. ("Boroditsky;" US 6,332,192). The Applicants have reviewed these references and respectfully assert that the present invention as recited in Claims 6-8 and 14-16 is not anticipated nor rendered obvious by Khan and Boroditsky, alone or in combination.

As presented above, Applicants respectfully submit that Khan does not show or suggest the present invention as recited in Claims 1 and 9. Claims 6-8 are dependent on Claim 1 and recite additional limitations, and Claims 14-16 are dependent on Claim 9 and recite additional limitations.

Boroditsky does not overcome the shortcomings of Khan. Applicants understand Boroditsky to only show a method of authenticating a user. As such, Applicants respectfully submit that Boroditsky, alone or in combination with Khan, does not show or suggest a method of activating a smart card. Specifically, Boroditsky, alone or in combination with Khan, does not show or suggest a "method of activating a smart card, comprising: receiving identifying information for a non-activated smart card; receiving manual authentication information for user to whom the non-activated

smart card has been issued; authenticating the user and the non-activated smart card using the identifying information and the manual authentication information; obtaining a public key from the non-activated smart card; and issuing a digital certificate that is generated using the public key, wherein the non-activated smart card is activated upon receiving the digital certificate," as recited in Claim 1.

In addition, Boroditsky, alone or in combination with Khan, does not show or suggest a "method of activating a smart card, comprising: sending, to an administration server, identifying information read from a non-activated smart card; sending, to the administration server, manual authentication information input by a user to whom the non-activated smart card has been issued; generating a public key using the non-activated smart card; sending the public key to the administration server; and receiving a digital certificate that is generated using the public key, wherein the non-activated smart card is activated upon receipt of the digital certificate," as recited in Claim 9.

In summary, Applicants respectfully submit that Khan and Boroditsky, alone or in combination, do not show or suggest the present invention as recited in independent Claims 1 and 9. As such, Applicants also respectfully submit that Claims 6-8 (dependent on Claim 1) and Claims 14-16 (dependent on Claim 9) are not shown or suggested by Khan and Boroditsky, alone or in combination. Therefore, Applicants respectfully submit that Claims 6-8 and 14-16 traverse the Examiner's basis for rejection

under 35 U.S.C. § 103(a) as these claims are dependent on allowable base claims and recite additional limitations.

Claims 23-25 are rejected under 35 U.S.C § 103(a) as being unpatentable over Khan in view of Boroditsky and Yacobi (US 5,872,844). The Applicants have reviewed these references and respectfully assert that the present invention as recited in Claims 23-25 is not anticipated nor rendered obvious by Khan, Boroditsky and Yacobi, alone or in combination.

Independent Claim 23 recites that an embodiment of the present invention is directed to a "method of activating then using a smart card, comprising: ... receiving identifying information for a non-activated smart card; receiving manual identification information for a user to whom the non-activated smart card has been issued; authenticating the user and the non-activated smart card using the manual authentication information and the identifying information; obtaining a public key from the non-activated smart card; and sending a digital certificate generated using the public key from a certificate authority to the non-activated smart card, wherein the non-activated smart card is activated upon receiving the digital certificate." Claims 24-25 are dependent on Claim 23.

Applicants respectfully assert that Khan does not show or suggest the present invention as recited in independent Claim 23. Applicants understand Khan to only describe the creation of a "digital identity" that perhaps can be used in a smart card. At best, the "digital identity" of Khan is possibly analogous to a digital certificate. However, as recited in the

claims, the present invention pertains to methods of activating a smart card. Applicants respectfully submit that Khan does not show or suggest a method of activating a smart card, and in particular does not show or suggest the method of activating a smart card recited by Claim 23.

Boroditsky does not overcome the shortcomings of Khan. Applicants understand Boroditsky to only show a method of authenticating a user. Applicants respectfully submit that Boroditsky, alone or in combination with Khan, does not show or suggest a method of activating a smart card. Specifically, Boroditsky, alone or in combination with Khan, does not show or suggest a method of activating a smart card as recited in Claim 23.

Yacobi does not overcome the shortcomings of Khan and Boroditsky. Applicants understand Yacobi to only show a method of detecting fraud. Applicants respectfully submit that Yacobi, alone or in combination with Khan and Boroditsky, does not show or suggest a method of activating a smart card. Specifically, Yacobi, alone or in combination with Khan and Boroditsky, does not show or suggest a method of activating a smart card as recited in Claim 23.

In summary, Applicants respectfully submit that Khan, Boroditsky and Yacobi, alone or in combination, do not show or suggest the present invention as recited in independent Claim 23, and that Claim 23 traverses the Examiner's basis for rejection under 35 U.S.C. § 103(a). Applicants also respectfully submit that Claims 24-25 (dependent on Claim 23) traverse the Examiner's basis for rejection under 35 U.S.C. § 103(a) as these claims are

dependent on an allowable base claim and recite additional limitations.

## CONCLUSION

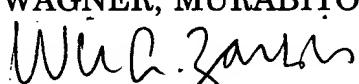
Based on the remarks and amendments presented above, Applicants request allowance of the present Application.

Based on the arguments presented above, Applicants respectfully assert that Claims 1-16 and 23-25 overcome the rejections of record and, therefore, Applicants respectfully solicit allowance of these Claims.

Applicants have reviewed the references that were cited but not relied upon. Applicants respectfully assert that the present claimed invention overcomes these references: US 5,120,939; US 5,799,086; US 6,327,659 and US 6,257,486.

The Examiner is invited to contact Applicants' undersigned representative if the Examiner believes such action would expedite resolution of the present Application.

Date: 3/18/03

Respectfully submitted,  
WAGNER, MURABITO & HAO LLP  
  
\_\_\_\_\_  
William A. Zarpis  
Reg. No. 46,120

Two North Market Street  
Third Floor  
San Jose, California 95113  
(408) 938-9060

VERSION WITH MARKINGS TO SHOW CHANGES MADE

IN THE CLAIMS

Please amend the claims as follows:

Please cancel Claims 17-22 without prejudice.

1. (Once Amended) A method of [using] activating a smart card, comprising:

[issuing a smart card to a user;

issuing manual authentication information to the user;]

receiving identifying information for a non-activated smart card;

receiving manual authentication information for user to whom the non-activated smart card has been issued;

authenticating the user and the non-activated smart card using the identifying information and the manual authentication information;

obtaining a public key from the non-activated smart card; and

issuing a digital certificate that is generated using the public key, wherein the non-activated smart card is activated upon receiving the digital certificate [to the smart card to activate the smart card].

2. (Once Amended) The method according to claim 1, wherein the manual authentication information comprises a user [ID] identifier and a password.

4. (Once Amended) The method according to claim 1, wherein

[the authenticating further comprises connecting] the smart card is connected to a workstation.

5. (Once Amended) The method according to claim 1, [further comprising storing] wherein the digital certificate is stored in at least one of the activated smart card and a workstation.

6. (Once Amended) The method according to claim 1, further comprising:

[connecting the smart card to a workstation;]

[initiating] receiving a login request [to a server] that is initiated when the activated smart card is connected to a workstation;

authenticating the activated smart card using the digital certificate; and

if authenticated, permitting a login to a computer resource.

7. (Once Amended) The method according to claim 6, wherein [the authenticating further comprises connecting the smart card to a workstation, and removing] the activated smart card is removed from the workstation after [the authenticating] it is authenticated.

8. (Once Amended) The method according to claim 6, wherein [the] authenticating the activated smart card further comprises determining that the digital certificate has not been revoked.

9. (Once Amended) A method of [using] activating a smart card,

comprising:

[receiving a smart card;  
receiving manual authentication information;  
authenticating the smart card using the manual authentication information;]  
sending, to an administration server, identifying information read from a non-activated smart card;  
sending, to the administration server, manual authentication information input by a user to whom the non-activated smart card has been issued;  
generating a public key using the non-activated smart card;  
sending the public key to [an] the administration server; and  
receiving a digital certificate that is generated using the public key.  
wherein the non-activated smart card is activated upon receipt of the digital certificate [to activate the smart card].

10. (Once Amended) The method according to claim 9, wherein the manual authentication information comprises a user [ID] identifier and a password.

12. (Once Amended) The method according to claim 9, wherein [the authenticating further comprises connecting] the smart card is connected to a workstation.

13. (Once Amended) The method according to claim 9, further comprising storing the digital certificate in at least one of the activated

smart card and a workstation.

14. (Once Amended) The method according to claim 9, further comprising:

connecting the activated smart card to a workstation;

sending a login request to a server[;]

[authenticating] that authenticates the digital certificate against a certificate revocation list; and

if authenticated, permitting a login to a computer resource.

15. (Once Amended) The method according to claim 14, wherein [the authenticating further comprises connecting the smart card to a workstation, and removing] the activated smart card is removed from the workstation after [sending] the digital certificate is sent.

16. (Once Amended) The method according to claim [9] 14, wherein the server determines [authenticating further comprises determining] that the digital certificate has not been revoked.

23. (Once Amended) A method of activating then using a smart card, comprising:

[issuing a smart card to a user;

issuing manual authentication information to the user, the manual authentication information comprising a user ID and a password;]

on first use of the smart card:

[connecting the smart card to a workstation;]

receiving identifying information for a non-activated smart card;  
receiving manual identification information for a user to  
whom the non-activated smart card has been issued;

authenticating the user and the non-activated smart card using  
the manual authentication information and the identifying information;

obtaining a public key from the non-activated smart card; and  
sending a digital certificate generated using the public key

from a certificate authority to the non-activated smart card, wherein  
the non-activated smart card is activated upon receiving the digital  
certificate [to activate the smart card.]; and

on a subsequent use of the smart card:

[connecting the smart card to a workstation;]

[sending] receiving a login request [to a server] that is initiated  
when the activated smart card is connected to a workstation;

authenticating the digital certificate against a certificate revocation  
list to determine that the digital certificate has not been revoked; and  
if authenticated, permitting a login to a computer resource.

24. (Once Amended) The method according to claim 23, wherein  
[the authenticating further comprises connecting] the activated smart card  
is connected to a workstation[,] and [the removing the smart card] removed  
from the workstation after [authenticating] it is authenticated.

25. (Once Amended) The method according to claim 23, [further  
comprising storing] wherein the digital certificate is stored in at least one of  
the activated smart card and a workstation.